

Arithmetically-free group-gradings of Lie algebras: II

Wolfgang Alexander Moens*

August 4, 2016

Abstract

We study Lie algebras L that are graded by an arbitrary group $(G, *)$ and have finite support, X . We show that L is nilpotent of $|X|$ -bounded class if X is arithmetically-free. Conversely: if a finite subset Y of G is *not* arithmetically-free, then Y supports the grading of a non-nilpotent Lie algebra.

Contents

1	Introduction	2
2	Arithmetically-free subsets of groups	4
3	Group-gradings of Lie algebras	4
3.1	Reduction to finite abelian grading groups	5
3.2	Group-gradings with non-arithmetically-free support	6
3.3	Lie-regularity of homogeneous words	7
3.4	Lie algebras with arithmetically-free support	9
4	A characterisation of arithmetically-free sets	9
4.1	Restrictions and shifts of alphabets	11
4.2	Regularity and Lie-regularity	11
4.3	Hyper-derivations and fullness	13
4.4	A recursive upper bound	14
4.5	Walks in Cayley-graphs	16

*This research was supported by the Erwin Schrödinger Junior Fellowship (Grant XXXX), and the Austrian Science Foundation FWF (Grant J3371-N25).

1 Introduction

In this paper we consider gradings of Lie algebras L by arbitrary groups $(G, *)$. We recall that such a grading is a decomposition $L := \bigoplus_{g \in G} L_g$ of L into homogeneous subspaces, such that for all $g, h \in G$, we have

$$[L_g, L_h] \subseteq L_{g*h}.$$

A typical example of such a grading is the eigenspace decomposition of L with respect to an automorphism or a derivation. Classical results in the literature conclude that, under reasonable conditions on the support $X := \{g \in G \mid L_g \neq \{0\}\}$ of the grading, the algebra L must be nilpotent (of bounded class). We refer to the bibliography for examples of, and partial answers to, the following questions:

Question 1.1. *Which properties of the support, X , guarantee that L is nilpotent, or nilpotent of $|X|$ -bounded class?*

Question 1.2. *Which properties of a set Y guarantee that it supports some non-nilpotent Lie algebra?*

In order to address these questions, we have introduced *arithmetically-free* subsets of groups, [16]. A subset X of an abelian group $(G, +)$ is arithmetically-free, iff X is finite and $x, x + y, x + 2y, x + 3y, \dots \subseteq X$ implies $y \notin X$. More generally: a subset X of an arbitrary group is arithmetically-free, iff X is finite and every subset of X of pairwise commuting elements is arithmetically-free. Perhaps the most obvious examples of arithmetically-free subsets of groups are subsets of $(\mathbb{Z}_p, +) \setminus \{\bar{0}\}$ and finite subsets of $(\mathbb{Z}^m, +) \setminus \{0\}$.

If we restrict our attention to gradings with finite support, then the answers to *Question 1.1* are given by theorem 3.14. We shall construct a *generalised Higman map* $H : \mathbb{N} \rightarrow \mathbb{N}$, such that:

Theorem (3.14). *Consider a Lie algebra L that is graded by a group G . If the support X of the grading is arithmetically-free, then L is nilpotent of class at most $H(|X|)$.*

We offer some context. If the Lie algebra is spanned by finitely-many elements, then the nilpotency follows from Jacobson's theorem about weakly-closed sets of nilpotent operators on finite-dimensional vector spaces, [8, 7]. If the Lie algebra is generated by finitely-many elements, then the nilpotency is a consequence of Zel'manov's theorem for Lie algebras satisfying a polynomial identity in the context of the restricted Burnside problem, [23]. We refer to remark 3.7 for more details.

Let us consider another special case – a result that extends Thompson's solution of the Frobenius conjecture. In [6], Higman proved the existence of a map $h : \mathbb{P} \rightarrow \mathbb{N}$ such that:

Theorem 1.3 (Higman). *Consider a Lie ring L that is graded by the simple group $(\mathbb{Z}_p, +)$. If the support does not contain $\bar{0}$, then L is nilpotent of class at most $h(p)$.*

We note that Higman used a combinatorial trick to prove the existence of the map $h : \mathbb{P} \rightarrow \mathbb{N}$, without providing an upper bound for $h(p)$. On the other hand: the generalised Higman map $H : \mathbb{N} \rightarrow \mathbb{N}$ will be the solution to an explicit recursion. It does indeed grow very quickly, but if we assume that the support of the grading also admits a good-ordering (in the sense of Shalev, [17]), then we obtain a stronger upper bound. In [16], we prove:

Theorem 1.4. *Consider a Lie algebra L that is graded by a group G . If the support X is arithmetically-free and admits a good-ordering, then L is nilpotent of class at most $1 + |X| + |X|^2 + |X|^3 + \dots + |X|^{2^{|X|}}$.*

In particular: we recover results by Kreknin-Kostrikin and Khukhro, [12, 9]. We refer to [16] for a more detailed exposition about arithmetically-free subsets of groups, and their applications to finite group theory and Lie theory.

We will deduce theorem 3.14 from the following characterisation of arithmetically-free subsets of groups.

Theorem (4.3). *Consider a finite subset X of an abelian group $(G, +)$, and let $<$ be a total order on G . Then the following two properties are equivalent:*

1. *The set X is arithmetically-free.*
2. *Every sequence $S = (g_1, g_2, \dots, g_{H(|X|)+1})$ on G of length $H(|X|) + 1$ has an initial segment (g_1, g_2, \dots, g_k) with $g_1 + g_2 + \dots + g_k \in G \setminus X$, or a Lie-regular segment $(g_i, g_{i+1}, \dots, g_j)$ with $g_i + g_{i+1} + \dots + g_j \in G \setminus X$.*

Lie-regularity is a minimality condition under the action of permutations derived from the Jacobi-identity; it will be introduced in *Definition 3*. We will prove the theorem by generalising the definitions and techniques of [6].

We also answer Question 1.2:

Proposition (3.8). *If a finite subset Y of a group G is not arithmetically-free, then there exists a non-nilpotent Lie algebra L that is graded by G such that the support is Y .*

Such a Lie algebra can be made to satisfy $\dim(L) = |Y|$ and $\text{dl}(L) = 2$. But there is a special Lie algebra, the standard filiform Lie algebra over a field \mathbb{F} , which characterises *all* (non)-arithmetically-free sets. This algebra is defined by the presentation, $\mathfrak{f} := \langle v, w_1, w_2, \dots \mid [v, w_i] = w_{i+1}, [w_j, w_k] = 0 \rangle$, where i, j and k run over all natural numbers.

Corollary (3.9). *A finite subset X of an arbitrary group is arithmetically-free, iff X does not support a grading of the standard filiform Lie algebra.*

Structure of the text. In section 2, we introduce arithmetically-free subsets of groups. In section 3, we prove the main results mentioned in the introduction modulo theorem 4.3. In section 4, prove theorem 4.3, which characterises arithmetically-free sets by means of Lie-regularity. We conclude with a remark about walks in Cayley-graphs.

2 Arithmetically-free subsets of groups

Let us begin by introducing some notation. For an element g of a group $(G, +)$, we let $\langle g \rangle$ be the cyclic subgroup of G that is generated by g . For elements $g, x \in G$ and $n \in \mathbb{N}$, we define the (partial) orbit, or (partial) arithmetic progression

$$\mathcal{O}_n(x, g) := \{x, x + g, x + 2 \cdot g, \dots, x + n \cdot g\},$$

with base x and increment g . The (full) orbit, or (full) arithmetic progression corresponding with x and g is $\mathcal{O}(x, g) := \{x, x + g, x + 2 \cdot g, x + 3 \cdot g, \dots\} = \bigcup_n \mathcal{O}_n(x, g)$.

Definition 2.1 (Arithmetically-free subsets). Consider an abelian group $(G, +)$ and a subset X of G . We say that X is arithmetically-free in G , iff X is finite and satisfies either (both) of the following properties:

1. If $x, g \in X$, then $\mathcal{O}(x, g) \not\subseteq X$,
2. If $x, g \in X$, then $\mathcal{O}_{|X|}(x, g) \not\subseteq X$.

More generally: a subset \tilde{X} of an arbitrary group $(\tilde{G}, *)$ is arithmetically-free, iff \tilde{X} is finite, and every subset X of pairwise commuting elements is arithmetically-free.

Example 2.2. Let $(G, *)$ be an arbitrary group and let X be a finite subset. If $\text{ord}_G(x) > |X|$ for every $x \in X$, then X is arithmetically-free. In particular:

1. Let $(\mathbb{Z}_n, +)$ be the cyclic group of order $n \in \mathbb{N}$. Then the subset $X := \{x \in \mathbb{Z}_n \mid \text{ord}_{(\mathbb{Z}_n, +)}(x) = n\}$ is arithmetically-free in $(\mathbb{Z}_n, +)$, and so are all subsets of X .
2. Let $(G, +)$ be the free-abelian group $(\mathbb{Z}^m, +)$ of rank $m \in \mathbb{N}$. Then the arithmetically-free subsets of G are precisely the *finite* subsets of $G \setminus \{0\}$.

Example 2.3. Let $(G, *)$ be an arbitrary group. If the finite subset X of G is sum-free, then X is arithmetically-free.

We refer to [16] for more examples and their applications.

3 Group-gradings of Lie algebras

In this section we will prove theorem 3.14 and propositions 3.8 and 3.9 modulo theorem 4.3. We begin by performing some elementary reductions.

3.1 Reduction to finite abelian grading groups

Suppose we are given a grading $\bigoplus_{g \in G} L_g$ of a Lie algebra L by a group G , with support X . If H is a subgroup of G , then we may define the homogeneous subalgebra

$$L_H := \bigoplus_{h \in H} L_h$$

of L , which is clearly graded by H , with support $X \cap H$. We note that if L is nilpotent of class at most $c \in \mathbb{N}$, then for every abelian subgroup H of G , the subalgebra L_H is nilpotent of class at most c . The following lemma from [16] shows that the converse is also true.

Lemma 3.1. *Consider $c \in \mathbb{N}$, an arbitrary group G , and a G -graded Lie algebra L with support X . The algebra L is nilpotent of class at most c , iff for every abelian subgroup H of G , the homogeneous H -graded subalgebra L_H of L with support $X \cap H$ is nilpotent of class at most c .*

So, in order to prove the nilpotency of graded Lie algebras, it suffices to consider abelian grading groups.

Definition 3.2 (Contraction). Consider two groups $(G, +)$ and $(H, +)$, with respective subsets X and Y . A contraction of X onto Y is a surjective map $f : X \rightarrow Y$ such that for all $x_1, x_2, x_3 \in X$ with $x_1 + x_2 = x_3$, we have $f(x_1) + f(x_2) = f(x_3)$.

Example 3.3. Every homomorphism is a contraction. A subset $X \subseteq (G, +)$ is sum-free, iff X contracts onto $\{\bar{1}\} \subseteq (\mathbb{Z}_2, +)$.

Contractions allow us to take a grading of a Lie algebra, and make the support smaller, or “less complicated.”

Proposition 3.4. *Consider a grading $\bigoplus_{g \in G} L_g$ of a Lie algebra L by the group $(G, +)$ with support X . If $f : X \rightarrow Y$ is a contraction of X onto $Y \subseteq (H, +)$, then*

$$L^y := \bigoplus_{x \in f^{-1}(y)} L_x \text{ for } y \in Y, \text{ and } L^h := \{0\} \text{ for all } h \in H \setminus Y$$

defines a grading of L by $(H, +)$ with support Y .

Proof. For arbitrary elements h, h' of H , we have

$$[L^h, L^{h'}] \subseteq \bigoplus_{\substack{x \in f^{-1}(h) \\ x' \in f^{-1}(h')}} [L_x, L_{x'}] \subseteq \bigoplus_{\substack{x \in f^{-1}(h) \\ x' \in f^{-1}(h')}} L_{x+x'} \subseteq L^{h+h'}. \quad \square$$

We note that much information may be lost in this construction. Indeed: the trivial homomorphism $\varepsilon : G \rightarrow H : x \mapsto 0$ shows that contractions need not map arithmetically-free sets onto arithmetically-free sets. We do have the following result.

Lemma 3.5. *Consider an abelian group $(G, +)$ and an arithmetically-free subset X . Then there exists a homomorphism $\pi : G \rightarrow H$ from G to a finite abelian group H such that $\pi(X)$ is arithmetically-free.*

Proof. Let G be given by $(\mathbb{Z}^m \oplus F, +)$, where $m \in \mathbb{N}$ and F is a finite abelian group. Since X is finite, there exists a natural number R such that for all $x := (x_1, \dots, x_m, x_{m+1}) \in X$: $0 < |x_1|, \dots, |x_m| < R/3$. Now define the natural projection $\pi : \mathbb{Z}^m \oplus F \rightarrow \mathbb{Z}_R^m \oplus F$. If $\pi(x) + \pi(y) = \pi(z)$, for some $x, y, z \in X$, then $R|(x_1 - y_1 - z_1), \dots, (x_m - y_m - z_m)$, so that $x = y + z$. In particular: if, for some $x, g \in X$ and $n \in \mathbb{N}$, we have $\mathcal{O}_n(\pi(x), \pi(g)) \in \pi(X)$, then we also have $\mathcal{O}_n(x, g) \in X$. \square

By combining proposition 3.4 with lemma ??, we obtain:

Corollary 3.6. *Consider a grading $\bigoplus_g L_g$ of a Lie algebra L by an abelian group G . Suppose that the support, X , is arithmetically-free. Then there exists a finite abelian group H and a grading of L by H such that the support, Y , is arithmetically-free and $|Y| \leq |X|$.*

So, when proving the nilpotency of graded Lie algebras with arithmetically-free support, we may assume that the grading group is finite and abelian. We can now explain the connection between theorem 3.14 and a result of Zel'manov.

Remark 3.7. Consider a graded Lie algebra L with arithmetically-free support X . Let us show that L is nilpotent if it is *finitely-generated*. By lemma 3.1, we may suppose that the grading group is abelian, and by corollary 3.6, we may even assume that it is finite abelian. Since X is arithmetically-free, the component L_0 satisfies a non-trivial polynomial identity. A result of Bahturin-Zaicev lifts this identity to a polynomial identity on all of L , [1]. Since L is finitely generated and X is finite, L is also generated by finitely many homogeneous elements. Since all homogeneous elements are ad-nilpotent of index at most $|X|$, we may apply Zel'manov's theorem to conclude that L is nilpotent, [23].

The theorems of Bahturin-Zaicev and Zel'manov have been extended (by Shumyatsky) to guarantee the existence of upper bounds for the degree of the polynomial identity and the nilpotency class, [20]. But, unfortunately, these bounds depend implicitly on the number of generators of L .

3.2 Group-gradings with non-arithmetically-free support

For each $n \in \mathbb{N}$, $n > 1$, we may define the standard metabelian Lie algebra $\mathfrak{m}(n)$ over a field \mathbb{F} by the presentation: $\mathfrak{m}(n) := \langle v, w_0, \dots, w_{n-1} | [v, w_i] = w_{i+1}, [w_j, w_k] = 0 \rangle$, where i, j, k run over the elements of $(\mathbb{Z}_n, +)$. Let us consider an obvious grading of $\mathfrak{m}(n)$. For any $g \in G$ of order n , and $x \in \text{Centr}_G(g) \setminus \langle g \rangle$, we define $\mathfrak{m}(n)_g := \mathbb{F} \cdot v$ and $\mathfrak{m}(n)_{x+i \cdot g} := \mathbb{F} \cdot w_i$, with $i \in \mathbb{Z}_n$. Then this extends to a G -grading of $\mathfrak{m}(n)$ with support $\mathcal{O}(x, g)$.

Proposition 3.8. *Consider a finite subset Y of a group $(G, *)$, and suppose that Y is not arithmetically-free. Then there exists a non-nilpotent Lie algebra L that is graded by G with support Y . It is metabelian and its dimension is $|Y|$.*

Proof. We may suppose that Y does not contain the neutral element of G (since otherwise every Lie algebra is supported by Y). Since Y is not arithmetically-free, there is a subset Y_0 of Y of pairwise commuting elements that is not arithmetically-free. So there exist $x, g \in Y_0$ with $\mathcal{O}(x, g) \subseteq Y_0 \subseteq Y$. Clearly, g has finite order $|\mathcal{O}(x, g)| - 1$, and $x \notin \langle g \rangle$. So $\mathfrak{m}(|\mathcal{O}(x, g)| - 1)$ is graded by G with support $\mathcal{O}(x, g) \subseteq Y$. The abelian Lie algebra $\mathbb{F}^{|Y| - |\mathcal{O}(x, g)|}$ is trivially graded by G with support $Y \setminus \mathcal{O}(x, g)$. So Lie algebra $L := \mathbb{F}^{|Y| - |\mathcal{O}(x, g)|} \oplus \mathfrak{m}(|\mathcal{O}(x, g)| - 1)$ is G -graded with support Y . It has dimension $|Y|$ and satisfies $[[L, L], [L, L]] = 0$. \square

Alternatively, we may consider the (infinite) standard filiform Lie algebra \mathfrak{f} over a field \mathbb{F} , which is given by the presentation $\mathfrak{f} := \langle v, w_1, w_2, \dots \mid [v, w_i] = w_{i+1}, [w_j, w_k] = 0 \rangle$, where i, j, k run over \mathbb{N} . This algebra is metabelian (but not nilpotent), and it also has obvious gradings. Let $g, x \in G$ be as before: g has order $n \in \mathbb{N}$ and $x \in G \setminus \langle g \rangle$. We define $\mathfrak{f}_g := \mathbb{F} \cdot v$, and for each $i \in \mathbb{N}$, we set $\mathfrak{f}_{x+i \cdot g} := \bigoplus_{j \geq 0} \mathbb{F} \cdot w_{i+j \cdot n}$. Then this extends to a G -grading of \mathfrak{f}_∞ with support $\mathcal{O}(x, g)$. As before, we obtain:

Proposition 3.9. *Consider a finite subset Y of a group G , and suppose that Y is not arithmetically-free. Then the standard filiform Lie algebra \mathfrak{f} has a G -grading with support $Y_0 \subseteq Y$.*

3.3 Lie-regularity of homogeneous words

In this subsection we introduce Lie-regular words, which turn out to be very useful in proving the nilpotency of graded algebras. We first recall some standard notation. If L is a Lie algebra, and $v_1, \dots, v_k, v_{k+1} \in L$, then we recursively define the left-associative products by $[v_1, \dots, v_k, v_{k+1}] := [[v_1, \dots, v_k], v_{k+1}]$. The bilinearity of the Lie-bracket together with the Jacobi-identity guarantee that every product of k elements can be written as a linear combination of left-associative products of length k . Let us make this precise.

Linearisations and Lie-regularity. Consider the free Lie algebra F with free generating set $u_1, \dots, u_k, v_1, \dots, v_l, w_1, \dots, w_m$. Let P be an arbitrary (not necessarily left-associative) product of the elements v_1, \dots, v_l , e.g.: $P = [[v_1, v_2], [v_3, v_4]]$ or $P = [v_1, [[v_2, v_3], v_4]]$. By applying the Jacobi-identity at most $(l-1)$ -times, we obtain a set of permutations $\mathcal{S}_P \subseteq \text{Sym}(l)$ containing the identity, a map $\varepsilon_P : \mathcal{S}_P \rightarrow \{\pm 1\}$, and the *linearisation* of P :

$$[u_1, \dots, u_k, P, w_1, \dots, w_m] = \sum_{\pi \in \mathcal{S}_P} \varepsilon_P(\pi) \cdot [u_1, \dots, u_k, v_{\pi(1)}, \dots, v_{\pi(l)}, w_1, \dots, w_m].$$

Example 3.10. Let $l := 4$, and $P := [[v_1, v_2], [v_3, v_4]]$. The linearisation of P is then given by the 8 permutations $\mathbb{1}, (12), (34), (12)(34), (13)(24), (1324), (1423), (14)(23)$ and their respective signs $+, -, -, +, -, +, +, -$.

Definition 3.11 (Lie-regularity). Let $(A, <)$ be a totally-ordered set, and give A^l the lexicographical order. The sequence $(a_1, \dots, a_l) \in A^l$ is *Lie-regular*, iff there exists a set of permutations \mathcal{S}_P defining the linearisation of a Lie product P , such that $(a_1, \dots, a_l) < (a_{\pi(1)}, \dots, a_{\pi(l)})$, for all $\pi \in \mathcal{S}_P \setminus \{\mathbb{1}\}$.

We briefly mention that it also makes sense to consider linearisations in Lie algebras that satisfy various identities, say: metabelian or solvable Lie algebras. The corresponding notion of regularity will then yield stronger conclusions (i.e.: explicit upper bounds for the nilpotency class). We refer to [16] for examples of such bounds.

Graded linearisation. The above linearisation formula holds in every Lie algebra. But, if the Lie algebra is graded, then the linearisations become more interesting. So let us consider a grading $\bigoplus_g L_g$ of a Lie algebra L by a finite abelian group $(G, +)$ and let $X \subseteq G$ be its support. Let $<$ be a total order on X , and extend it lexicographically to all finite X -tuples.

We define the homogenous, left-associative words (of the grading) to be the homogeneous elements v_1, v_2, \dots themselves, and their iterated products $[v_1, v_2], [v_1, v_2, v_3], \dots$. To every homogeneous element v that is not zero, we may associate a unique element $\bar{v} \in X$ such that $v \in L_{\bar{v}}$. If the elements v_1, \dots, v_k are homogeneous and not zero, then we assign to the word $[v_1, v_2, \dots, v_k]$ the weight sequence $(\bar{v}_1, \dots, \bar{v}_k) \in X^k \subseteq G^k$. If $[v_1, v_2, \dots, v_k]$ and $[w_1, w_2, \dots, w_l]$ are two such words, we may compare them:

$$[v_1, v_2, \dots, v_k] < [w_1, w_2, \dots, w_l] \leftrightarrow (\bar{v}_1, \dots, \bar{v}_k) < (\bar{w}_1, \dots, \bar{w}_l).$$

Let us evaluate the identity $(*)$ in homogeneous elements of the grading $\bigoplus_g L_g$. Suppose that $v_1, \dots, v_k \neq 0$, but $\bar{v}_1 + \dots + \bar{v}_l \in G \setminus X$. Then $P = 0$, so that the identity collapses to

$$0 = \sum_{\pi \in \mathcal{S}_P} \varepsilon_P(\pi) \cdot [u_1, \dots, u_k, v_{\pi(1)}, \dots, v_{\pi(l)}, w_1, \dots, w_m].$$

We have (trivially) shown:

Proposition 3.12. *Consider a non-zero, left-associative, homogeneous word v with weight sequence $(a_1, \dots, a_k, b_1, \dots, b_l, c_1, \dots, c_m) \in X^{k+l+m}$. If the segment (b_1, \dots, b_l) is Lie-regular and $b_1 + \dots + b_l \in G \setminus X$, then v is spanned by strictly larger, left-associative, homogeneous words of the same length.*

Similarly, we obtain:

Proposition 3.13. *Consider non-zero, homogeneous elements $v_1, \dots, v_k, w_1, \dots, w_l$. If $\bar{v}_1 + \dots + \bar{v}_k \in G \setminus X$, then $[v_1, \dots, v_k, w_1, \dots, w_l] = 0$.*

3.4 Lie algebras with arithmetically-free support

We are now in a position to prove theorem 3.14 modulo theorem 4.3.

Theorem 3.14. *Consider a Lie algebra L that is graded by a group G . If the support, X , of the grading is arithmetically-free, then L is nilpotent of class at most $H(|X|)$.*

Proof. Let the grading be given by $L = \bigoplus_{g \in G} L_g$. In view of lemma 3.1, we may assume that G is abelian. Let \mathcal{W} be the set of non-zero, left-associative, homogeneous words (w.r.t this grading) of length $H(|X|)+1$. Let $(X, <)$ be an arbitrary total order on X , and order all elements of \mathcal{W} by their weight sequences. Suppose $\mathcal{W} \neq \emptyset$. Since there are only finitely many sequences on X of length $H(|X|) + 1$, we may assume that $W \in \mathcal{W}$ is maximal. Let S be the weight sequence of W . If S has an initial segment with weight in $G \setminus X$, then W vanishes according to proposition 3.13. This contradicts the choice of W . If S has a Lie-regular segment of weight in $G \setminus X$, then according to proposition 3.12, W is a linear combination of $W' \in \mathcal{W}$, with $W' > W$. Since W was chosen maximal-non-zero, all of the W' vanish. This again contradicts the choice of W . But theorem 4.3 guarantees that one of these cases must occur. We conclude $\mathcal{W} = \emptyset$, so that L is nilpotent of class at most $H(|X|)$. \square

We recall some notation: the lower central series of a Lie algebra L is defined by $\gamma_1(L) := [L, L]$, and $\gamma_{t+1} := [\gamma_t(L), L]$ for $t \in \mathbb{N}$, $t > 1$.

Corollary 3.15. *Consider a Lie algebra L that is graded by a group G . Let X be an arithmetically-free subset of G and let I be a homogeneous ideal of L containing the homogeneous subspace $\bigoplus_{g \in G \setminus X} L_g$ of L . Then $\gamma_{H(|X|)+1}(L) \subseteq I$.*

4 A characterisation of arithmetically-free sets

Definition 4.1 (Alphabet, weight). An *alphabet* with coefficients in an abelian group $(G, +)$ is a totally ordered set $(A, <)$ together with a map $\omega : A \rightarrow G$, called the *weight*, and an arithmetically-free subset X of G . Notation: $(A, <, \omega : A \rightarrow G, X)$, or simply $(A, <, \omega, X)$. We say that the alphabet is *finite*, if $\omega^{-1}(X)$ is a finite subset of A .

In 4.19, we recursively define a map $H : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} : (a, b, c) \mapsto H_a(b, c)$. The main aim of this section is to prove the following theorem.

Theorem 4.2. *Consider a finite alphabet $(A, <, \omega : A \rightarrow G, X)$, and let $S := (a_1, \dots, a_k)$ be a sequence on A of length $k \geq H_{|X|}(|X|, |\omega^{-1}(X)|)$. Then $\{0, \omega(a_1), \omega(a_1) + \omega(a_2), \dots, \omega(a_1) + \dots + \omega(a_k)\} \subseteq G$ cannot be translated into X , or S contains a Lie-regular segment (a_i, \dots, a_j) with $\omega(a_i) + \dots + \omega(a_j) \in G \setminus X$.*

We recall that a subset M of G can be translated into a subset N of G , iff there exists an $h \in G$ such that $h + M := \{h + m | m \in M\} \subseteq N$. Set $H(n) := H_n(n, n)$. If we specialise $A := G$ and $\omega : A \rightarrow G : a \mapsto a$, then we obtain:

Theorem 4.3 (Characterisation of arithmetically-free subsets of groups). *Consider an abelian group $(G, +)$ with total order $<$ and a finite subset X . The following two properties are then equivalent:*

1. *X is arithmetically-free.*
2. *Every sequence $S := (g_1, g_2, g_3, \dots, g_k)$ on G of length $k \geq H(|X|) + 1$, has an initial segment (g_1, g_2, \dots, g_l) satisfying $g_1 + g_2 + \dots + g_l \in G \setminus X$, or has a Lie-regular segment $(g_i, g_{i+1}, \dots, g_j)$ satisfying $g_i + g_{i+1} + \dots + g_j \in G \setminus X$.*

Proof. Suppose first that X is arithmetically-free, and let $S := (g_1, \dots, g_k) \in G^k$, with $k \geq H(|X|) + 1$. Define the $T := (g_2, \dots, g_k) \in G^{H(|X|)}$. If $\{0, g_2, g_2 + g_3, \dots, g_2 + \dots + g_k\}$ cannot be translated into X , then neither can $g_1 + \{0, g_2, g_2 + g_3, \dots, g_1 + \dots + g_k\} = \{g_1, g_1 + g_2, \dots, g_1 + \dots + g_k\}$. Else, theorem 4.2 gives us a Lie-regular segment $U := (g_i, \dots, g_j)$ of T (and therefore of S) satisfying $g_i + \dots + g_j \in G \setminus X$.

Conversely, suppose that X is not arithmetically-free. Then there exist $x, g \in X$ with $\mathcal{O}(x, g) \subseteq X$. For each $k \in \mathbb{N}$, we define $S_k := (x, g, \dots, g) \in X^{k+1}$. It is now easy to verify that the S_1, S_2, \dots form a family of arbitrarily long sequences on G for which every initial and every Lie-regular segment $T := (a_1, \dots, a_l)$ satisfies $a_1 + \dots + a_l \in X$. Indeed: the initial segments of S_k are S_1, \dots, S_k . If $x < g$, then the Lie-regular segments are again precisely S_1, S_2, \dots, S_k . Else, S_k has no Lie-regular segments at all. \square

This was the theorem used to prove theorem 3.14. If we specialise even more ($G := \mathbb{Z}_p$, for some prime p , and $X := \mathbb{Z}_p \setminus \{0\}$), then we recover the central result (lemma 3) of [6]. In particular: $h(p) \leq H(p - 1)$, for all primes p .

Before sketching the proof of theorem 4.2, we present some useful invariants.

Definition 4.4 (Weight, Span, Content). Consider a finite alphabet $(A, <, \omega, X)$, and let $S := (a_1, \dots, a_k)$ be a sequence on A . The *weight* of S is $\omega_1(S) := \omega(a_1) + \dots + \omega(a_k)$. The *span* of S is $\sigma(S) := \{0, \omega(a_1), \omega(a_1) + \omega(a_2), \dots, \omega(a_1) + \dots + \omega(a_k)\} \subseteq G$. We also define $\alpha(S) := \omega^{-1}(X) \cap \{a_1, \dots, a_k\} \subseteq A$. The *content* of S is $\kappa(S) := (|\sigma(S)|, |\alpha(S)|) \in \mathbb{N} \times \mathbb{N}$.

Let us *informally* define a sequence $S := (a_1, \dots, a_k) \in A^k$ on A to be *full*, if S satisfies the conclusions of theorem 4.2 in a particularly strong sense. (For a more precise definition, we refer to 4.10 and 4.9).

Strategy of the proof. This will be a (relatively simple) induction on the type of the sequence. Let us give $\mathbb{N} \times \mathbb{N}$ the lexicographical order $<_{\text{Lex}}$, and let us fix a finite alphabet $\mathcal{A} := (A, <, \omega, X)$. Let us first show that a finite sequence S on A satisfying $\|S\| \geq H_{|X|}(\kappa(S))$ is full. If $\kappa(S) \in \mathbb{N} \times \{1\}$ or $\{1\} \times \mathbb{N}$, or if $|\sigma(S)| > |X|$,

then S will be full for trivial reasons. In the other case, we construct a new finite alphabet $\mathcal{A}' := (A', <', \omega' : A' \rightarrow G, X)$, and a new sequence S' on A' such that:

1. If S' is full (w.r.t. \mathcal{A}'), then S is full (w.r.t. \mathcal{A}),
2. $\kappa(S') <_{\text{Lex}} \kappa(S)$, and
3. $\|S'\| \geq H_{|X|}(\kappa(S'))$.

The induction step then yields the above claim. By construction, the map $H_{|X|} : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is monotone increasing in both arguments. Now suppose that $\|S\| \geq H_{|X|}(|X|, |\omega^{-1}(X)|)$. If $|\sigma(S)| \leq |X|$, then S is full by the above. Else, $|\sigma(S)| > |X|$, so that S is trivially full. This finishes the proof.

4.1 Restrictions and shifts of alphabets

Definition 4.5 (Restriction). Consider a finite alphabet $\mathcal{A} := (A, <, \omega : A \rightarrow G, X)$ and a subset A' of A . Let $<'$ be the restriction of $<$ to A' , and let $\omega' : A' \rightarrow G$ be the restriction of ω to A' . Then we say that the finite alphabet $(A', <', \omega' : A' \rightarrow G, X)$ is the *restriction* of \mathcal{A} to A' .

If A is a set, we define $W^0(A) := A$, and we let $W(A) : W^1(A)$ be the set of finite sequences on A . Inductively, we then define $W^{n+1}(A) := W(W^n(A))$, for all $n \in \mathbb{N}$. We also define

$$W^*(A) := \bigcup_{n \geq 0} W^n(A).$$

The length $\|S\|$ of an element $S := (x_1, \dots, x_k) \in W^{n+1}(A)$, with $x_1, \dots, x_k \in W^n(A)$, is defined to be k .

Definition 4.6 (Shift). Consider a finite alphabet $\mathcal{A} := (A, <, \omega : A \rightarrow G, X)$. Let $<_1$ be the lexicographical order on $W(A)$, and define $\omega_1 : W(A) \rightarrow G : (x_1, \dots, x_k) \mapsto \omega(x_1) + \dots + \omega(x_k)$. Then $(W(A), <_1, \omega_1, X)$ is again an alphabet, the *shift* of \mathcal{A} . By iteration, we obtain a family of alphabets $(W^n(A), <_n, \omega_n, X)_{n \in \mathbb{N}}$. For $S := (x_1, \dots, x_k) \in W(W^n(A))$, we define the *span* to be $\sigma(S) := \omega_n(x_1) + \dots + \omega_n(x_k)$.

4.2 Regularity and Lie-regularity

We recall that Lie-regularity was defined by means of identities (linearisations) in the free Lie algebra. It is possible, and it will be convenient, to define a family Lie-regular elements by combinatorial means, and without having to invoke permutations. This will be the family of (simply) regular elements with respect to a fixed alphabet.

Definition 4.7 (Regularity and type). Consider an alphabet $\mathcal{A} := (A, <, \omega, X)$. All elements of $W^0(A) = A$ are regular and of the same type. Now let $n \in \mathbb{N} \cup \{0\}$. An element (x_1, \dots, x_k) of $W^{n+1}(A)$, with $x_1, \dots, x_k \in W^n(A)$, is regular, iff

1. The elements x_1, \dots, x_k are all regular, and
2. The elements x_1, \dots, x_k are all of the same type, and
3. $\exists 1 \leq l < k$ such that $x_1 = x_2 = \dots = x_l <_n x_{l+1}, \dots, x_k$.

Two regular elements (x_1, \dots, x_k) and (y_1, \dots, y_l) of $W^{n+1}(A)$ are of the same type, iff $x_1 = y_1$.

Definition 4.8 (Underlying sequence). Let $(A, <)$ be a totally-ordered set. We define the family $(\pi_n : W^{n+1}(A) \longrightarrow W^n(A))_{n \geq 0}$ of maps by

$$\pi_n(((x_1, \dots, x_k), \dots, (z_1, \dots, z_m))) := (x_1, \dots, x_k, \dots, z_1, \dots, z_m) \in W^n(A).$$

We further define the map $\pi : W^*(A) \longrightarrow W(A)$, by: for all $S \in W^n(A)$,

$$\begin{aligned} \pi(S) &:= \pi_1 \circ \dots \circ \pi_{n-1}(S) \in W(A) \text{ if } n \geq 2, \\ \pi(S) &:= S \text{ if } n = 1, \\ \pi(S) &:= (S) \text{ if } n = 0. \end{aligned}$$

The *underlying sequence* of an element $S \in W^*(A)$ is defined to be $\pi(S) \in W(A)$.

Lemma 4.9 (Regularity implies Lie-regularity). *Consider an alphabet $\mathcal{A} := (A, <, \omega, X)$. If an element $S \in W^{n+1}(A)$ is regular, then the underlying sequence of S is Lie-regular.*

Proof. We refer to lemma 6 of [6] for the proof. It inducts on $n \geq 0$, and it implicitly constructs the set $\mathcal{S}_P \subseteq \text{Sym}(r)$ and the map $\varepsilon_P : \mathcal{S}_P \longrightarrow \{\pm 1\}$. \square

This observation, together with theorem 4.3, inspires us to define fullness.

Definition 4.10 (Fullness). Consider an alphabet $\mathcal{A} := (A, <, \omega, X)$. A sequence $S := (a_1, \dots, a_k) \in A^k$ on A is *full*, iff: (1) $\sigma(S)$ cannot be translated into X , or (2) some segment T of S is the underlying sequence of a regular element of $W^*(A)$ with $\omega_1(T) \in G \setminus X$.

Example 4.11. Consider an alphabet $\mathcal{A} := (A, <, \omega, X)$ and the elements $a < b < c$ in A . We define the sequences $R := (a, b, c)$, $S := (a, a, b)$, $T := (a, b, b)$ and $U := (a, a, a)$ on X . Then R, S, T are trivially regular, while U trivially fails to be regular. Let F be a free Lie algebra with free generating set x, x_1, x_2, x_3 of F . Define $P := [x_1, [x_2, x_3]]$ and $Q := [[x_1, x_2], x_3]$. The Jacobi-identity then gives the linearisations:

$$\begin{aligned} [x, P] &= [x, x_1, x_2, x_3] - [x, x_1, x_3, x_2] - [x, x_2, x_3, x_1] + [x, x_3, x_2, x_1], \\ [x, Q] &= [x, x_1, x_2, x_3] - [x, x_2, x_1, x_3] - [x, x_3, x_1, x_2] + [x, x_3, x_2, x_1]. \end{aligned}$$

So $\mathcal{S}_P := \{\mathbb{1}, (23), (123), (13)\}$ and $\mathcal{S}_Q := \{\mathbb{1}, (12), (132), (13)\}$. We see that S is Lie-regular because of the first identity, and that T is Lie-regular because of the second identity. Also: either identity guarantees that R is Lie-regular. Since U is constant, every permutation will fix U . We conclude that U is not Lie-regular.

4.3 Hyper-derivations and fullness

Definition 4.12 (Derivations and hyper-derivations). Consider a finite alphabet $(A, <, \omega, X)$. A *derivation* of an element $S \in W(A)$ is a regular element $T \in W^2(A)$ such that the underlying sequence $\pi(T)$ of T is a segment of S . We say that T is a *hyper-derivation* of S , iff in addition $|\sigma(T)| < |\sigma(S)|$.

In particular: if T is a hyper-derivation of S , then $\kappa(T) <_{\text{Lex}} \kappa(S)$.

Lemma 4.13. Consider an alphabet \mathcal{A} and its shift \mathcal{B} . Let S be a finite sequence on \mathcal{A} , and let T be a derivation of S . If T is full w.r.t. \mathcal{B} , then S is full w.r.t. \mathcal{A} .

Proof. Note that $\sigma(T)$ can be translated into $\sigma(S)$. Note also that a regular segment U of T (w.r.t. \mathcal{B}) is a derivation of S , with the same weight as its underlying sequence (w.r.t. \mathcal{A}). \square

Let us now construct these hyper-derivations.

Lemma 4.14 (Existence of obvious derivations). Consider an alphabet $(A, <, \omega, X)$ and an element $S := (a_1, \dots, a_k) \in W(A)$. Let $a := \min\{a_1, \dots, a_k\}$. Suppose that there exist natural numbers $1 \leq i_1 < j_1 < i_2 < j_2 < \dots < i_s < j_s \leq k$ such that for all $t \in \{1, 2, \dots, s\}$: $a_{i_t} = a$ and $a_{j_t} > a$. Then S has a derivation of length s .

Proof. This is a simple induction on $s \in \mathbb{N}$. \square

Definition 4.15. We define the family of functions $(f_n)_{n \in \mathbb{N}} : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ to be the unique solution of the recurrence relation $f_n(\alpha + 1, \lambda) = \lambda \cdot (f_n(\alpha, \lambda) + n)$, with initial conditions $f_n(1, \lambda) := n$. We also define the map $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} : (\alpha, \lambda) \longmapsto \lambda \cdot \alpha^\lambda$.

Although we will not be needing the exact solution of this recurrence, we can mention that the maps $f_n(\alpha, \lambda)$ are a polynomial in λ of degree $\alpha - 1$: $f_n(\alpha, \lambda) = n \cdot (\lambda^{\alpha-1} + \sum_{1 \leq j \leq \alpha-1} \lambda^j)$. We note that for all $u, v, w \in \mathbb{N}$, $f_w(u, v) \leq w \cdot f(v, u)$. Also: the number of sequences of length at most v on u letters is at most $f(u, v)$.

Lemma 4.16. Consider a finite alphabet $\mathcal{A} := (A, <, \omega, X)$ and sequence $S \in W(A)$. If $\sigma(S)$ can be translated into X , then $|\sigma(S)| \leq |X|$, and $\sigma(S)$ does not contain $\mathcal{O}_{|X|}(x, y)$ with $x \in G$ and $y \in X$.

Proof. (1). This follows from the fact that translations of subsets in G preserve cardinality. (2). If $\mathcal{O}_{|X|}(x, y) \subseteq \sigma(S)$, then $\mathcal{O}_{|X|}(u + x, y) \subseteq u + \sigma(S)$. \square

Lemma 4.17 (Existence of derivations). Consider a finite alphabet $(A, <, \omega, X)$ and an element $S := (a_1, \dots, a_k) \in W(\omega^{-1}(X))$ such that $\sigma(S)$ can be translated into X . If there is an $l \in \mathbb{N}$ with $k \geq f_{|X|}(|\sigma(S)|, l)$, then S has a derivation of length l .

Proof. We may suppose that $k = f_{|X|}(|\alpha(S)|, l)$. Let proceed by induction on $\alpha := |\alpha(S)|$. If $\alpha = 1$, then $a_1 = \dots = a_k$, and $\mathcal{O}_{|X|}(0, a_1) \subseteq \sigma(S)$. This contradicts our assumption. Now suppose that $\alpha > 1$. Then there exist $S_1, \dots, S_l \in W(\alpha(S))$ of length $f_{|X|}(\alpha - 1, l)$, and $T_1, \dots, T_l \in W(\alpha(S))$ of length $|X|$, such that

$$S = \pi_1((S_1, T_1, S_2, T_2, \dots, S_l, T_l)).$$

If some S_j does not use all letters of $\alpha(S)$, then we may use the induction hypothesis. Else, every S_j uses every letter of $\alpha(S)$. Then $y := \min \alpha(S)$ occurs in every S_j . If any of the $\pi_1((S_j, T_j))$ is constant, then $\sigma(S)$ contains an orbit $\mathcal{O}_{|X|}(u, v)$, with $v \in X$. This contradicts our assumption on $\sigma(S)$. So we may apply *Lemma 4.14* to conclude that S has a derivation of length l . \square

Proposition 4.18 (Existence of hyper-derivations). *Consider a finite alphabet $(A, <, \omega, X)$ and an element $S := (a_1, \dots, a_k) \in W(\omega^{-1}(X))$ such that $\sigma(S)$ can be translated into X . If $k \geq |X| \cdot f(|\omega^{-1}(X)|, |X| + l + 1)$, for some $l \in \mathbb{N}$, then S a hyper-derivation of length at least l .*

Proof. The map $f_{|X|}$ is monotone in its first argument, and $|\alpha(S)| \leq |\omega^{-1}(X)|$. The previous lemma then guarantees the existence of a derivation $T := (t_1, t_2, \dots, t_{|X|+l}, t_{|X|+l+1})$ of S of length $|X| + l + 1$. Note that the elements t_1, t_2, \dots are all regular of the same type. So we may suppose that they are all of the form (y, \dots) , for some fixed $y \in \omega^{-1}(X)$. Define $U := (t_1, \dots, t_{|X|+l}) \in W^2(\omega^{-1}(X))$. If $t_1 = t_2 = \dots = t_{|X|+l}$, then $\sigma(T)$ contains an orbit of the form $\mathcal{O}_{|X|}(r, t_1)$, with $t_1 \in X$. Then also $\sigma(S)$ contains such an orbit, and this contradicts our assumption. So U is a regular element of $W^2(\omega^{-1}(X))$.

Note that $\sigma(U) \subseteq \sigma(T)$ and $|\sigma(T)| \leq |\sigma(S)|$. Suppose that $\sigma(U) = \sigma(T)$. If $u \in \sigma(U) = \sigma(T)$, then also $u + y \in \sigma(T) = \sigma(U)$. We conclude that $\sigma(U), \sigma(T)$ and $\sigma(S)$ contain an orbit of the form $\mathcal{O}(r, y)$. This contradicts our assumption on $\sigma(S)$. We conclude that $|\sigma(U)| < |\sigma(S)|$. \square

4.4 A recursive upper bound

Definition 4.19 (Generalised Higman-map). We define a map $H : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} : (a, b, c) \mapsto H_a(b, c)$ by the boundary conditions $H_a(1, c) := 1$, $H_a(b, 1) := a$ and, for $b, c > 1$, by the recursion

$$H_a(b, c) := \max \{ a \cdot f(c, a + H_a(b - 1, a \cdot f(c - 1, H_a(b, c - 1))) + 1, \\ H_a(b - 1, c), H_a(b, c - 1) \}.$$

By specialisation, we obtain the maps $H : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} : (m, n) \mapsto H_m(m, n)$ and $H : \mathbb{N} \rightarrow \mathbb{N} : n \mapsto H_n(n, n) = H(n, n)$. The latter is called the *generalised Higman map*.

By construction: if $b' \leq b$ and $c' \leq c$, then $H_a(b', c') \leq H_a(b, c)$.

Theorem 4.20 (Fullness, conditional on the content). *Consider a finite alphabet $\mathcal{A} := (A, <, \omega : A \longrightarrow G, X)$ and $S \in W(A)$. If $\|S\| \geq H_{|X|}(\kappa(S))$, then S is full.*

Proof. Let S be given by (a_1, \dots, a_k) , and let us prove the statement by induction on the content, $\kappa(S) \in (\mathbb{N} \times \mathbb{N}, <_{\text{Lex}})$, of S . In order to simplify the formulae, we abbreviate $\sigma := |\sigma(S)|$ and $\alpha := |\alpha(S)|$. Suppose first that $\sigma = 1$. Then $k \geq 1$, and (a_1) is a regular segment of weight in $G \setminus X$, so that S is full. Suppose next that $\alpha = 1$. Then $k \geq |X|$, and $\mathcal{O}_{|X|}(a_1, a_1) \subseteq \sigma(S)$. If $\omega(a_1) \in X$, then $\sigma(S)$ contains an orbit with increment in X , so that S is full. If $\omega(a_1) \in G \setminus X$, then (a_1) is a regular element of weight in $G \setminus X$, so that again S is full. We may therefore assume that $\sigma, \alpha > 1$.

We may assume even more: the letters a_1, \dots, a_k of S are all in $\omega^{-1}(X)$, and $\sigma(S)$ can be translated into X , since otherwise S is trivially full. We may then apply proposition 4.18, and obtain a hyper-derivation $U := (x_1, \dots, x_l) \in W(W(\alpha(S)))$ of S with length $l \geq H_{|X|}(\sigma - 1, r)$, where $r := |X| \cdot f(\alpha - 1, H_{|X|}(\sigma, \alpha - 1))$. We may assume that none of the x_j is full, since otherwise S is again trivially full.

In order to complete the induction, we need only find a subset B of $W(A)$ of size $|B| \leq r$ such that $U \in W(B)$. Indeed: the finite alphabet $\mathcal{B} := (B, <', \omega' : B \longrightarrow G, X)$ is a restriction of a shift of \mathcal{A} , so that lemma 4.13 applies. By definition, there is a $y \in \alpha(S)$ such that each x_i is in $W(\{y\}) \times W(\alpha(S) \setminus \{y\}) \subseteq W(A)$. Let B be the set of regular elements of $W(A)$ in $W(\{y\}) \times W(\alpha(S) \setminus \{y\})$ that are not full and that have type at most (σ, α) . The elements x_1, \dots, x_l all belong to B , so that indeed $U \in W(B)$.

Let $Y \in B$. Then it is of the form $Y = \pi((Y_H, Y_T))$, with $Y_H \in W(\{y\})$ and $Y_T \in W(\alpha(S) \setminus \{y\})$. Since Y is not full, neither is Y_H . Since $\alpha(Y_H) = 1$, we have $\|Y_H\| < H_{|X|}(\kappa(Y_H)) := |X|$. Similarly: since Y is not full, neither is Y_T . Since $\kappa(Y_T) <_{\text{Lex}} \kappa(Y)$, we may apply the induction hypothesis to obtain $\|Y_T\| < H_{|X|}(\kappa(Y_T))$. Since $\sigma(Y_T) \leq \sigma$ and $\alpha(Y_T) \leq \alpha - 1$, we get $\|Y_T\| \leq H_{|X|}(\sigma, \alpha - 1)$. We see that each $Y \in B$ draws from $|X|$ -many heads and $H_{|X|}(\sigma, \alpha - 1)$ -many tails, and conclude that $|B| \leq r$. This finishes the proof. \square

Proof. (Of theorem 4.3) If $|\sigma(S)| > |X|$, then S is full for trivial reasons. Else, $|\sigma(S)| \leq |X|$ and $|\alpha(S)| \leq |\omega^{-1}(X)|$. Then $\kappa(S) \leq_{\text{Lex}} (|X|, |\omega^{-1}(X)|)$, and

$$\|S\| \geq H(|X|, |\omega^{-1}(X)|) := H_{|X|}(|X|, |\omega^{-1}(X)|) \geq H_{|X|}(\kappa(S)).$$

Theorem 4.20 guarantees that S is full. Lemma 4.9 then completes the proof. \square

4.5 Walks in Cayley-graphs

Our results can also be stated in the language of Cayley-graphs. Let us consider the Cayley-graph $\Gamma := \Gamma(G, X)$ of $(G, +)$ with respect to X . For every finite walk $W := (v_1, v_2, \dots, v_{n+1})$ in Γ , we define its sequence of edges to be

$$E(W) := (v_2 - v_1, v_3 - v_2, \dots, v_{n+1} - v_n) \in X^n.$$

We define the walk W to be (Lie)-regular, iff $E(W)$ is (Lie)-regular. We obtain:

Corollary 4.21. *If X is arithmetically-free, then every sufficiently long walk in $X \subseteq \Gamma(G, X)$ contains a (Lie)-regular walk from a to b with $b - a \notin X$. In particular: every sufficiently long walk in $\mathbb{Z}_p^\times \subseteq \Gamma(\mathbb{Z}_p, \mathbb{Z}_p^\times)$ contains a Lie-regular cycle.*

Thanks. The author would like to thank his host, Efim Zel'manov, and Lance Small for their hospitality during the Erwin Schrödinger Research Programme (*Representations and gradings of solvable algebras: 2013 – 2015, J3371 – N25*) at the University of California, San Diego. He would also like to express his gratitude to the Erwin Schrödinger International Institute for Mathematical Physics where preliminary work for the research was done (*Lie algebras: deformations and representations*). Finally, he thanks the Geometric and Analytic Group Theory-group of the University of Vienna.

References

- [1] BAHTURIN, Y. A.; ZAICEV, M. V.: Identities of graded algebras. J. Algebra 205 (1998), no. 1, 1-12.
- [2] BENKART, G.; KOSTRIKIN, A. I.; KUZNETSOV, M. I.: Finite-dimensional simple Lie algebras with a nonsingular derivation. J. Algebra 171 (1995), no. 3, 894-916.
- [3] BERGEN, J.; GRZESZCZUK, P.: Gradings, derivations, and automorphisms of nearly associative algebras. J. Algebra 179 (1996), no. 3, 732-750.
- [4] BOREL, A.; SERRE, J.-P.: Sur certains sous-groupes des groupes de Lie compacts.: Comment. Math. Helv. 27, (1953). 128-139.
- [5] BURDE, D.; MOENS, W. A.: Periodic derivations and prederivations of Lie algebras J. Algebra 357 (2012), 208-221.
- [6] HIGMAN, G.: Groups and rings having automorphisms without non-trivial fixed elements J. London Math. Soc. 32 (1957), 321-334.
- [7] JACOBSON, N. Une généralisation du théorème d'Engel. C. R. Acad. Sci. Paris 234, (1952). 579-581.

- [8] JACOBSON, N.: A note on automorphisms and derivations of Lie algebras. Proc. Amer. Math. Soc. 6, (1955). 281-283.
- [9] KHUKHRO, E. I. Finite groups of bounded rank with an almost regular automorphism of prime order. Sibirsk. Mat. Zh. 43 (2002), no. 5, 1182–1191; translation in Siberian Math. J. 43 (2002), no. 5, 955-962
- [10] KHUKHRO, E. I.; MAKARENKO, N.; SHUMYATSKY, P.: Nilpotent ideals in graded Lie algebras and almost constant-free derivations Comm. Algebra 36 (2008), no. 5, 1869-1882.
- [11] KOSTRIKIN, A. I.; KUZNETSOV, M. I.: Two remarks on Lie algebras with nondegenerate derivation. Trudy Mat. Inst. Steklov. 208 (1995), Teor. Chisel, Algebra i Algebr. Geom., 186-192.
- [12] KREKNIN, V. A.; KOSTRIKIN, A. I.: Lie algebras with regular automorphisms. (Russian) Dokl. Akad. Nauk SSSR 149 1963 249-251.
- [13] MATTAREI, S.: The orders of nonsingular derivations of modular Lie algebras. Israel J. Math. 132 (2002), 265-275.
- [14] MATTAREI, S. The orders of nonsingular derivations of Lie algebras of characteristic two. Israel J. Math. 160 (2007), 2340.
- [15] MATTAREI, S. : A sufficient condition for a number to be the order of a nonsingular derivation of a Lie algebra. Israel J. Math. 171 (2009), 1-14.
- [16] MOENS, W.A.: Arithmetically-free group-gradings of Lie-algebras: I, *Preprint*.
- [17] SHALEV, A.: Automorphisms of finite groups of bounded rank. Israel J. Math. 82 (1993), no. 1-3, 395-404.
- [18] SHALEV, A.: The structure of finite p-groups: effective proof of the coclass conjectures. Invent. Math. 115 (1994), no. 2, 315-345.
- [19] SHALEV, A.: The orders of nonsingular derivations. Group theory. J. Austral. Math. Soc. Ser. A 67 (1999), no. 2, 254-260.
- [20] SHUMYATSKY, P.: Applications of Lie ring methods to group theory. Nonassociative algebra and its applications (So Paulo, 1998), 373-395, Lecture Notes in Pure and Appl. Math., 211, Dekker, New York, 2000.
- [21] SHUMYATSKY, P.; TAMAROZZI, A.; WILSON, L.: \mathbb{Z}_n -graded Lie rings. J. Algebra 283 (2005), no. 1, 149-160.
- [22] Thompson, J.: Finite groups with fixed-point-free automorphisms of prime order. Proc. Nat. Acad. Sci. U.S.A. 45 1959 578-581.
- [23] Zel'manov, E.I.: Lie algebras and torsion groups with identity. *Preprint*, <https://arxiv.org/abs/1604.05678>.